UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,188	04/20/2007	Glenn Mansfield Keeni	8075-1100	6594

466 7590 12/21/2010

YOUNG & THOMPSON
209 Madison Street
Suite 500
Alexandria, VA 22314

EXAMINER	
VICTORIA, NARCISO F	
ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
12/21/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

DocketingDept@young-thompson.com

Office Action Summary	Application No.	Applicant(s)	
	10/588,188	KEENI, GLENN MANSFIELD	
	Examiner	Art Unit	
	NARCISO VICTORIA	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 October 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *10-22,24 and 25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *10-22,24 and 25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the communication filed on October 6, 2010. Claims 10-22 and 24-25 are pending of which claims 10, 13, 20 and 24 are independent and the remainder dependent. Applicant amended all independent and dependent claims, cancelling claims 23 and 26 in addition to previously cancelled claims 1-9.

Response to Arguments

2. In the "Remarks" filed on October 6, 2010, Applicant's arguments and amendments with respect to the rejection of claims 10-22 and 24-25 have been fully considered and are persuasive. However, further search yielded additional prior art (Apap et al., US 7,448,084) that Examiner believes meets the limitation "the number of distinct values" argued by the Applicant on pages 10-12 of the "Remarks." The Examiner further believes that when the prior art Chesla already employing the use of "ratios" in detecting an attack (see at least paragraph [0029]) is combined with Apap and Chao would render the instant invention obvious; hence, at this time, the Examiner believes that the rejection of claims 10-22 and 24-25 should be maintained. Additionally, further review of the instant application resulted in additional claim objections and rejections as set forth below.

Examiner's Note

4. While particular columns and line numbers in the prior art references are cited and applied against the claims by the Examiner in an Office action, it is done so for the

convenience of the Applicant(s). Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures in the prior art references may apply as well. It is respectfully requested that, in preparing responses, the Applicant(s) fully consider the prior art references in their entirety as potentially teaching all or part of the claimed invention as well as the context of the passages taught by the prior art or disclosed by the Examiner.

Claim Objections

5. Claims 10 and 15-20 are objected to because of the following informalities:

on line 32 of claim 10, the word --or-- needs to be added after the semi-colon and before condition (d) since the four conditions (a through d) are written in the alternative;

on line 1 of claims 15-19, for consistency, the word "tracking" needs to be replaced by --detection--;

on line 29 of claim 20, the comma after the word "progress" needs to be changed to a --semi-colon (;)-- to be followed by the word --or-- instead of "and" since the four conditions (a through d) are written in the alternative; additionally, there's a missing colon (:) after the word "satisfied" on line 10; and conditions a-b also need to end with a semi-colon vice a comma.

In addition, since the four conditions of claims 10 and 20 are written in the alternative, all variables should be defined within each condition or prior to all the conditions (for example, "based on one of the following conditions where "N(t)" is a

number of distinct values observed, "P(t)" is a number of packets in transmission, etc...then start listing or enumerating the alternative conditions).

Appropriate corrections are required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 10 and 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

On line 12 of claim10, using the introductory phrase "based on one of the following conditions", four conditions (a through d) are written in the alternative, meaning each condition should be able to stand on its own and yet condition (c) is written to depend on (b) "if the ratio of the coefficient computed in (b)" (line 28), making the claim unclear or indefinite.

Similar problem is found in claim 20 where condition (c) is written to depend on (b) "if the ratio of the coefficient computed in (b)" (line 25).

Also, claims 10 and 20 recite the limitation "the coefficient computed in (b)" in line 28 and 25 respectively. There is insufficient antecedent basis for this limitation in the claim since there is no "coefficient" mentioned in (b).

Claim Rejections - 35 USC § 101

8. 35 U.S.C. § 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

9. Claims 10-19 are rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter.

As to independent claim 10, this claim when read in light of the specification, can be interpreted as being directed toward program/software per se. Applicant is reminded that a program and/or software cannot be patentable. Independent claim 10 recites a "system" performing a series of steps but reciting no element that is a physical part of a device. When a system claim, in at least one possible way, can be implemented by software alone and the claim does not contain any element that is a physical part of a device, the claim must be rejected under 35 U.S.C. §101 as non-statutory since the claim does not fall under one of the four statutory categories of invention (Process, Machine, Manufacture or Composition of Matter).

Dependent claims 11-12 and 15-17 do not recite nor impart any further limitations that would bring the invention in conformance with 35 U.S.C. §101 as patentable subject matter.

Similarly, independent claim 13 recites a "system" but recites not a single element that is a physical part of a device and the claim, when read in light of the specification, can be interpreted as being directed to a program and/or software. When a system claim, in at least one possible way, can be implemented by software alone and the claim does not contain any element that is a physical part of a device, the claim

must be rejected under 35 U.S.C. §101 as non-statutory since the claim does not fall under one of the four statutory categories of invention (Process, Machine, Manufacture or Composition of Matter).

Dependent claims 14 and 18-19 do not recite nor impart any further limitations that would bring the invention in conformance with 35 U.S.C. §101 as patentable subject matter.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. § 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 13-14 and 24-25 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Chesla et al. (US 2004/0250124; hereinafter Chesla) in view of Apap et al. (US 7,448,084; hereinafter Apap).

As per claim 13, Chesla discloses a network attack detection system, wherein it is judged that an illegal attack has taken place by observing the values of the packet header fields (**see at least Para. [0023], lines 5-8: performing statistical analysis on one or more packet header fields to detect an attack**).

Chesla does not specifically disclose:

"and when the number of distinct values seen in a combination of two or more header fields exceeds a pre- specified threshold value within a pre-specified time, it is judged that an attack is in progress."

However, Apap discloses **that statistics gathered in observing how many distinct values occur in a monitored feature and compared against a model of normal usage in a registry access system can be used in detecting malicious activity** (**Col. 12, lines 51-60**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and incorporate Apap to meet the preceding limitation not explicitly disclosed by Chesla. The motivation is to detect if an access is malicious (**Apap: Col. 12, line 45**).

As per claim 14, Chesla in view of Apap discloses the network attack detection system according to claim 13, wherein the judgment is made that an attack is in progress, if the Time to Live (TTL) value in the header of the packet does not lie in the range of the values seen beforehand for the source address in the header of the packet (**see at least Chesla, Para. [0045]: one of the header fields that is monitored is time-to-live (TTL) when detecting an attack**).

As per claim 24, Chesla discloses a method for detecting a network attack, comprising the step of:

observing values of packet header fields (**see at least Para. [0023], lines 5-8: performing statistical analysis on one or more packet header fields to detect an attack**).

Chesla does not explicitly disclose:

"and upon observing that a number of distinct values seen in a combination of two or more header fields exceeds a pre-specified threshold value within a pre-specified time, judging that an unauthorized attack is in progress."

However, Apap discloses **that statistics gathered in observing how many distinct values occur in a monitored feature and compared against a model of normal usage in a registry access system can be used in detecting malicious activity** (**Col. 12, lines 51-60**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and incorporate Apap to meet the preceding limitation not explicitly disclosed by Chesla. The motivation is to detect if an access is malicious (**Apap: Col. 12, line 45**).

As per claim 25, Chesla in view of Apap discloses the method of claim 24, wherein a Time To Live (TTL) value in the packet header is observed, and the unauthorized attack in progress is judged upon the observed TTL value being outside a range of the values seen beforehand for the source address in the packet header (**see at least Para. [0025-0026]; [0045]: for example, as part of measuring a property of traffic entering the network and applying a fuzzy logic algorithm to detect an**

attack; packet header fields that are monitored include time-to-live (TTL), source IP address, packet size, and so on).

12. Claims 10-12, 15-17 and 20-22 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Chesla in view of Apap and further in view of Chao et al. (US 7,526,807; hereinafter Chao).

As per claim 10, Chesla discloses a network attack detection system, comprising the steps of:

examining a header of a packet in transmission (**see at least Para. [0023], lines 5-8: performing statistical analysis on one or more packet header fields**);

observing values of one or more pre-specified fields in the packet header (**Para. [0045]: for example, TTL field, source IP address field, etc**).

Chesla does not explicitly disclose:

"and in a case where a number of distinct values observed in the pre-specified fields reaches a pre-specified threshold within a pre-specified time interval, judging that an unauthorized attack is in progress."

However, Apap discloses **that statistics gathered in observing how many distinct values occur in a monitored feature and compared against a model of normal usage in a registry access system can be used in detecting malicious activity** (**Col. 12, lines 51-60**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and incorporate Apap to meet the

preceding limitation not explicitly disclosed by Chesla. The motivation is to detect if an access is malicious (**Apap: Col. 12, line 45**).

Chesla in view of Apap does not explicitly disclose:

"wherein the judging is carried out based on one of the following conditions:

(a) N(t) is the number of distinct values of the field observed within a pre-specified time interval from time t, $N(t_1)$ is the number of distinct values of the field observed within the pre-specified time interval from some time t_1 and if the ratio of N(t) to $N(t_1)$ is greater than or equal to a first pre-specified threshold k_1, that is, if $N(t)/ N(t_1) \geq k_1$, the system will judge that an attack is in progress;

(b) P(t) is the number of packets in transmission within the pre-specified time interval from time t, and if the ratio of the number of N(t) to P(t) is greater than or equal to a second pre-specified threshold k_2, that is, $N(t)/P(t) \geq k_2$, the system will judge that an attack is in progress;

(c) $P(t_1)$ is the number of packets in transmission within the pre-specified time interval from some time t_1, and if the ratio of the coefficient computed in (b) above for the time t to that computed for the time t_1, $\{N(t)/P(t)\} / \{N(t_1)/P(t_1)\}$, is greater than or equal to a third pre-specified threshold k_3, that is, $\{N(t)/P(t)\} / \{N(t_1)/P(t_1)\} \geq k_3$, the system will judge that an attack is under progress;

(d) T(t) is the number of octets or bits in the packets in transmission within the pre-specified time interval from some time t, and if the ratio N(t) to T(t) is greater than or equal to a fourth pre-specified threshold k_4, that is, $N(t)/T(t) \geq k_4$, the system will judge that an attack is in progress."

However, Chao discloses, in one embodiment, DCS 108 performing aggregation function 222 by comparing measured attribute values to nominal attribute values, wherein if the measured attribute value exceeds a predetermined threshold, DCS 108 may conclude that the packets are suspect, as in part of an attack (**see at least Figure 5 and Col. 9, lines 30-38: as stated by Chao's disclosure, one skilled in the art would appreciate that various thresholds and combinations thereof may be used to determine whether packets are suspect**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and incorporate Chao to meet the preceding limitations not explicitly disclosed by Chesla and Apap. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

As per claim 11, Chesla in view of Apap and Chao discloses the network attack detection system according to claim 10, wherein arbitrary combinations of two or more header fields are allowed, and the number of distinct values observed for the resultant composite field is used to compute the coefficient which is compared against the threshold (**see at least Chesla: Para. [0025-0026]: for example, as part of measuring a property of traffic entering the network and applying a fuzzy logic algorithm to detect an attack**).

As per claim 12, Chesla in view of Apap and Chao discloses the network attach detection system according to claim 10, wherein an illegal attack is inferred to be underway when the Time To Live (TTL) value in the header field of a packet does not lie in the range of the values seen beforehand for the source address in the header of packets (**see at least Chesla: Para. [0045]: one of the header fields that is monitored is time-to-live (TTL) when detecting an attack**) .

As per claim 15, Chesla in view of Apap discloses the network attack tracking system according to claim 10.

Chesla in view of Apap does not explicitly disclose:

"wherein a source of the unauthorized attack is searched by deploying these systems at various places on the Internet."

However, Chao discloses denial-of-service control servers that are distributed in a given network to form a system configured to protect against DDoS attack (**see at least Fig. 1 and Col. 3, lines 56-67**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and Apap and incorporate Chao such that the system as being characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

As per claim 16, Chesla in view of Apap and Chao discloses the network attack tracking system according to claim 11.

Chesla in view of Apap does not explicitly disclose:

"wherein a source of the unauthorized attack is searched by deploying these systems at various places on the Internet."

However, Chao discloses denial-of-service control servers that are distributed in a given network to form a system configured to protect against DDoS attack (**see at least Fig. 1 and Col. 3, lines 56-67**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and Apap and incorporate Chao such that the system as being characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

As per claim 17, Chesla in view of Apap and Chao discloses the network attack tracking system according to claim 12.

Chesla in view of Apap does not explicitly disclose:

"wherein a source of the unauthorized attack is searched by deploying these systems at various places on the Internet."

However, Chao discloses denial-of-service control servers that are distributed in a given network to form a system configured to protect against DDoS attack (**see at least Fig. 1 and Col. 3, lines 56-67**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and Apap and incorporate Chao such that the system as being characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

As per claim 20, Chesla discloses a method for detecting a network attack, comprising the steps of:

examining a pre-specified field in a header of a packet in transmission for distinct values (**see at least Para. [0023], lines 5-8: performing statistical analysis on one or more packet header fields**).

Chesla does not explicitly disclose:

"and determining that an unauthorized attack is in progress based on an observed number of distinct values in the examined pre-specified header field reaching a pre-specified threshold within a pre-specified time interval."

However, Apap discloses **that statistics gathered in observing how many distinct values occur in a monitored feature and compared against a model of**

normal usage in a registry access system can be used in detecting malicious activity (**Col. 12, lines 51-60**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and incorporate Apap to meet the preceding limitation not explicitly disclosed by Chesla. The motivation is to detect if an access is malicious (**Apap: Col. 12, line 45**).

Chesla in view of Apap does not explicitly disclose:

"wherein, the determination includes that at least one of the following conditions is satisfied

(a) N(t) is the number of the distinct values of the field observed within the pre-specified time interval from some time t, $N(t_1)$ is the number of distinct values of the field observed within the pre-specified time interval from some time t_1 and if the ratio of N(t) to $N(t_1)$ is greater than or equal to a first pre-specified threshold k_1, that is $N(t)/N(t_1) \geq k_1$, it will be judged that an attack is in progress,

(b) P(t) is the number of packets in transmission within the pre-specified time interval from some time t, and if the ratio of N(t) to P(t) is greater than or equal to a second pre-specified threshold k_2, that is, $N(t)/P(t) \geq k_2$, it will be judged that an attack is in progress,

(c) $P(t_1)$ is the number of packets in transmission within the pre-specified time interval from the time t_1, and if the ratio of the coefficient computed in (b) above for the time t to that computed for the time t_1, $\{N(t)/P(t)\} / \{N(t_1)/P(t_1)\}$, is greater than or equal to

a third pre-specified threshold k_3, that is, $\{N(t)/P(t)\} / \{N(t_1)/P(t_1)\} \geq k3$, it will be judged that an attack is in progress, and

(d) T(t) is the number of octets or bits in the packets in transmission within the pre-specified time interval from some time t, and if the ratio N(t) to T(t) is greater than or equal to a fourth pre-specified threshold k_4, that is, $N(t)/T(t) \geq k_4$, it will be judged that an attack is in progress."

However, Chao discloses, in one embodiment, DCS 108 performing aggregation function 222 by comparing measured attribute values to nominal attribute values, wherein if the measured attribute value exceeds a predetermined threshold, DCS 108 may conclude that the packets are suspect, as in part of an attack (**see at least Figure 5 and Col. 9, lines 30-38: as stated by Chao's disclosure, one skilled in the art would appreciate that various thresholds and combinations thereof may be used to determine whether packets are suspect**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and Apap and incorporate Chao to meet the preceding limitations not explicitly disclosed by Chesla and Apap. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

As per claim 21, Chesla in view of Apap and Chao discloses the method of claim 20, wherein,

said examining step examines a resultant composite field comprising arbitrary combinations of two or more of header fields, and the number of distinct values observed for the resultant composite field is used to compute the coefficient which is compared against the threshold (**see at least Chesla: Para. [0025-0026]: for example, as part of measuring a property of traffic entering the network and applying a fuzzy logic algorithm to detect an attack**).

As per claim 22, Chesla in view of Apap and Chao discloses the method of claim 20, comprising the further steps of: from an examined packet, inferring that the unauthorized attack is underway when a Time To Live (TTL) value in the pre-specified field of the examined packet is outside a range of the values seen beforehand for the source address in the header of the examined packet, and after determining that the source address in the header of the examined packet is legitimate, detecting the unauthorized attack based on whether the TTL value is within a pre-specified range of the expected TTL value for the source address (**see at least Chesla: Para. [0025-0026]; [0045]: for example, as part of measuring a property of traffic entering the network and applying a fuzzy logic algorithm to detect an attack; packet header fields that are monitored include time-to-live (TTL), source IP address, packet size, and so on**).

13. Claims 18-19 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Chesla in view of Apap as applied to claims 13 and 14 above, and further in view of Chao.

As per claim 18, Chesla in view of Apap discloses the network attack tracking system according to claim 13.

Chesla in view of Apap does not explicitly disclose:

"wherein a source of the unauthorized attack is searched by deploying these systems at various places on the Internet."

However, Chao discloses denial-of-service control servers that are distributed in a given network to form a system configured to protect against DDoS attack (**see at least Fig. 1 and Col. 3, lines 56-67**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and Apap and incorporate Chao such that the system as being characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

As per claim 19, Chesla in view of Apap discloses the network attack tracking system according to claim 14.

Chesla in view of Apap does not explicitly disclose:

"wherein the source of the unauthorized attack is searched by deploying these systems at various places on the Internet."

However, Chao discloses denial-of-service control servers that are distributed in a given network to form a system configured to protect against DDoS attack (**see at least Fig. 1 and Col. 3, lines 56-67**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and Apap and incorporate Chao such that the system as being characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to Applicant's disclosure:

Lyon (US 7,478,429) - this reference discloses system and method for detecting and mitigating network overload.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to NARCISO VICTORIA whose telephone number is (571)270-7904. The examiner can normally be reached on Monday to Friday 10:00am - 6:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/NV/
/Taghi T. Arani/
Supervisory Patent Examiner, Art Unit 2438